# NEC Express5800 Fault Tolerant Virtual Server Quick Start Guide

## Install and Configure NEC Fault Tolerant Servers to Provide Maximum Availability to Virtual Server 2005 R2 SP1

For the latest information, please see

http://www.necam.com/servers/ft/ and http://www.microsoft.com/virtualserver

# Contents

## Introduction

Welcome to your Quick Start Guide to configuring Microsoft Virtual Server 2005 R2 Service Pack 1 (SP1) on an NEC Corporation of America Express5800 Fault Tolerant Server (FT Server) platform. NEC designs and builds servers that provide the highest level of reliability and performance for your Virtual Server 2005 R2 SP1 solution. The FT Server provides built-in fault tolerance for your virtualized environment, so you can enjoy the benefits of virtualization, including:

- Hardware consolidation
- Optimal hardware resource usage
- Separation of applications
- Flexible operating environment

This Guide will provide you with the necessary steps to install and configure hardware and software components for your virtual environment. In addition, the Guide will outline a solution scenario that provides you with the necessary information to deploy virtual solutions by using FT Servers and Microsoft Virtual Server 2005 R2 SP1 in production environments.

Your first task is to prepare the server hardware for installation of the host operating system. How you configure your hardware and create the fault tolerant environment is critical to the success of your solution.

This Guide takes you through the following procedures:

- Installing the server hardware
- Configuring Windows Server 2003 Enterprise Edition
- Configuring the hardware
- Installing Virtual Server 2005 R2 SP1
- Configuring the virtual machines

Because the Guide uses a scenario to provide a context for the information, there are a number of assumptions made regarding the operating environment. The next section describes these assumptions.

## Quick Start Guide Operating Environment

FT Servers provide optimal fault tolerance and performance for a number of server roles and IT services. When combined with Virtual Server 2005 R2 SP1, a single FT Server can operate a number of these roles and services concurrently. This Guide walks you through the process of creating this type of virtualized operating environment.

This Guide makes the following assumptions about your current network environment:

- You want to install the FT Server specifically for the deployment of Microsoft Virtual Server R2 SP1 and virtual machines, and you do not want to run any other applications.
- You will deploy the virtual servers to a branch office. The branch office has good connectivity to the main office and runs infrastructure and application services including one each of the following:
    - Domain controller;
    - File server; and
    - Exchange 2003 mail server.

*Currently, NEC FT systems do not support 64-bit applications so the email virtual machine will run Exchange 2003 instead of Exchange 2007.*

    - You install Virtual Server 2005 R2 SP1 on Windows Server 2003 SP1 or later. There are no extra services or applications running on the Virtual Server Host.

This Guide makes the following assumptions about the environment into which you deploy the FT Server:

- You do not have any other servers running Windows on your network. (You can have other Windows servers on your network, but they are not required.)
- You are installing Virtual Server 2005 R2 SP1 on Windows Server 2003 R2.
- Your servers are members of an Active Directory environment.
- You install Microsoft Exchange Server 2003 Service Pack 2 (SP2) or later.
- You configure Exchange Server 2003 as a stand-alone server, not as part of a Windows cluster.
- You install the Microsoft Virtual Machine PCI SCSI Controller driver on the guest operating system.
- You do not enable the virtual hard disk Undo feature.

**Guide Scenario**

The scenario for the Guide includes three physical servers that provide infrastructure and application services.

Figure 1 shows the initial environment.

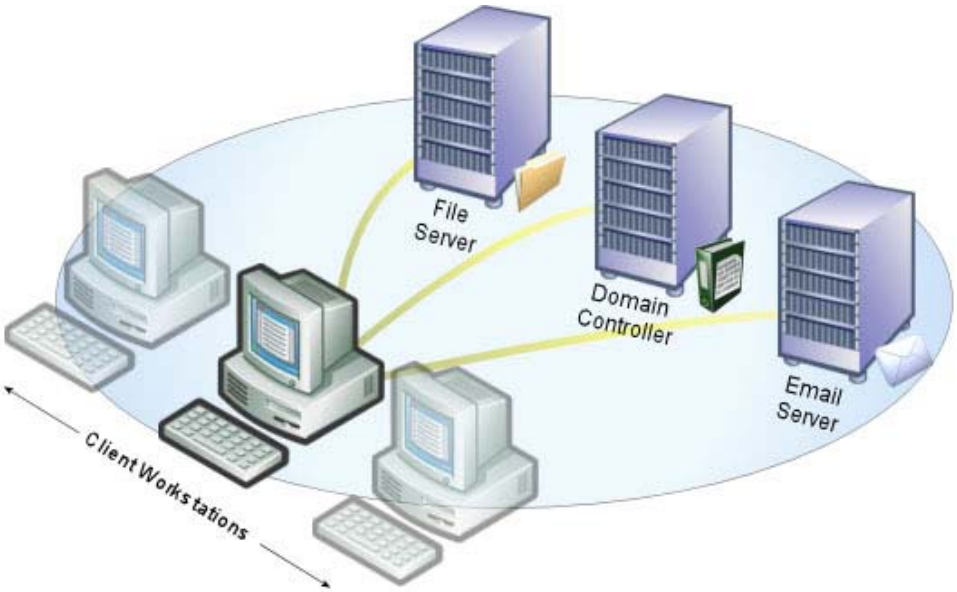



**Figure 1: Initial environment.**

You will deploy virtual machines to replace these physical servers. This enables you to use Virtual Server to address cost, reliability, management, and performance issues.

The virtualization solution uses three virtual machines (domain controller, file server, and email server) which will run on the FT Server.

Figure 2 shows the target virtual environment.

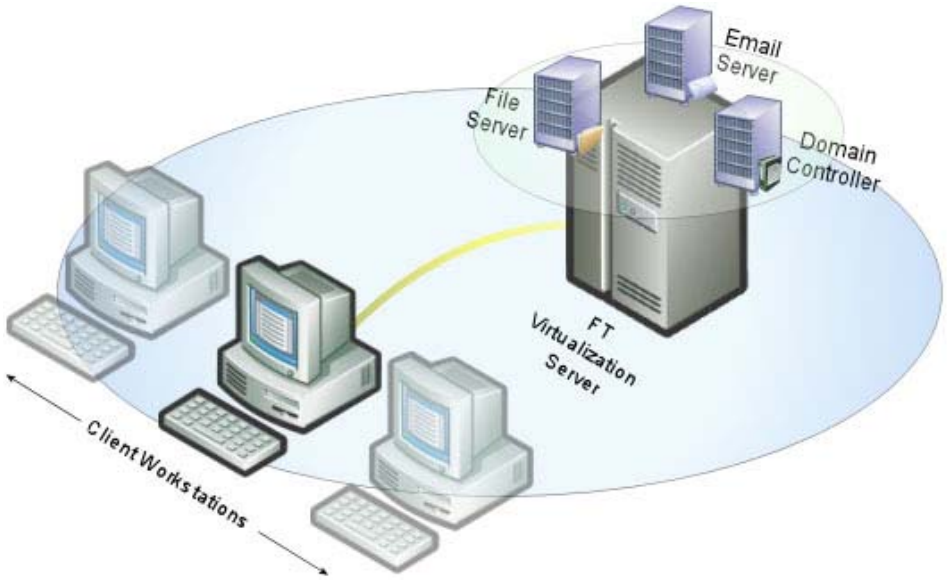



**Figure 2: Virtual environment.**

## Guide Goal

The goal of this Guide is to get you started as quickly as possible. It does not go into detailed explanations or descriptions of FT Server technologies or Virtual Server 2005 R2 SP1 features and capabilities.

If you want to learn more about the capabilities of FT Servers, you can read more on the NECAM website:

http://support.necam.com/servers/ft

If you want to learn more about the capabilities of Microsoft Virtual Server R2 SP1, you can read more on the Microsoft website:

http://www.microsoft.com/virtualserver

To set up your Virtual Server solution in a high availability configuration, you must perform the following five steps:

- **STEP 1:** Install the hardware
- **STEP 2:** Install the operating system
- **STEP 3:** Configure the server hardware
- **STEP 4:** Install and configure Virtual Server 2005 R2 SP1
- **STEP 5:** Install and configure the guest virtual machines

The rest of this Quick Start Guide walks you through each of these steps.

# STEP 1: Install the Hardware

You must ensure that you have the necessary hardware to create your virtual machine solution and that you have installed it correctly. Infrastructure solutions that use Microsoft Virtual Server 2005 R2 SP1 run multiple virtual machines on a single physical server. Because this type of solution runs multiple servers on a single piece of hardware, it is important to make sure that you configure the hardware correctly.

An FT Server provides your virtual solution with hardware fault tolerance and performance. To use the fault tolerance built into the NEC servers, you must configure the hardware components correctly. Specifically, to provide redundancy for network connectivity, you must install multiple network adapters. In addition, to maintain operation in the event of a power outage, you must configure the power inputs correctly.

## Connecting to the Network

All of the virtual machines that run on the server rely on the same network connectivity for client connection to the services and applications that the virtual machines provide. Because a failure in the network connectivity of the server has an impact on a large amount of network functionality, you must include fault tolerance for network connections.

To provide fault tolerance for network connections and to enhance performance, configure the network adapters into teams. In a network adapter team, one adapter is the primary or active adapter and all other adapters are secondary or backup adapters.

If the active adapter fails in a *fault tolerant* team, the backup adapter becomes active and seamlessly continues operation. In a *performance* team, network traffic distributes between the adapters. In addition to increasing performance, a performance team can also provide fault tolerance if an adapter fails.

You are going to create an Adapter Fault Tolerant (AFT) team. The Guide describes the configuration of AFT teams in *STEP 3: Configure the Server Hardware.* For now, we are going to connect the network adapters to the network and create an AFT team.

To connect the embedded Ethernet controllers to the network:

1. Provide an **unshielded twisted pair (UTP)** cable with **RJ-45 connectors** for each of the four **Ethernet** adapters.
2. Install the **Ethernet** adapters in **pairs**, one in the same numbered slot in each **module**. For example, for the **first team**, install an adapter in slot one in each **module**.
3. Connect one end of each cable to a network port on the **server** and the other end to a **switch**.

The following sections explain the different types of network adapter teams.

### Adapter Fault Tolerant Teams

An AFT team is a set of two or more network adapters that provide redundant connections to a single switch. In an AFT team, a single adapter is active on the network until a failover occurs (usually caused by failure of the adapter); at this point, a secondary adapter becomes active.

In an AFT team, both adapters connect to the same switch. Therefore, if the switch fails, both adapters become unavailable, and network connectivity is lost.

Figure 3 shows an AFT configuration and the outcome of adapter and switch failure.

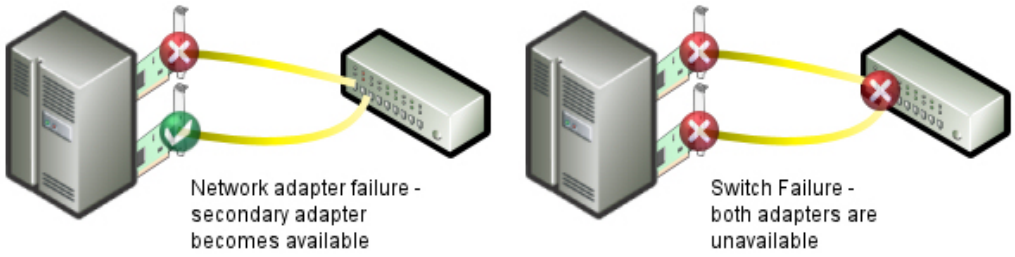



**Figure 3: Outcome of adapter and switch failure with AFT.**

### Switch Fault Tolerant Teams

A Switch Fault Tolerant (SFT) team is similar to an AFT team, except that SFT enables you to connect the team members to separate switches for increased fault tolerance. An SFT team must contain only two network adapters, and you must connect each adapter to a different switch that supports the Spanning Tree Algorithm. As in an AFT team, the primary adapter is active on the network. The secondary adapter becomes active after adapter failover, which usually occurs because the primary adapter fails or if its link to the switch fails.

In a SFT team, each adapter connects to a different switch; this configuration can continue operation if a switch fails.

Figure 4 shows the SFT configuration and the outcome of adapter and switch failure.

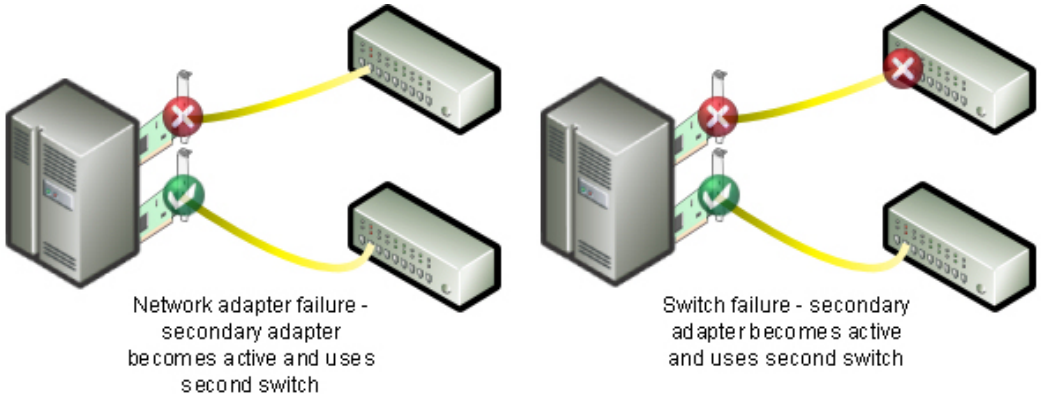



**Figure 4: Outcome of adapter and switch failure with SFT.**

### Adaptive Load Balancing Teams

In an Adaptive Load Balancing (ALB) team, both the primary and secondary adapters transmit data to provide an increase in performance. However, only the primary adapter receives data. To prevent packet-order problems, one adapter in an ALB team transmits all packets to a particular destination. In addition, only the primary adapter transmits broadcast packets and non-Internet Protocol (IP) packets. You must connect all adapters in an ALB team to the same switch or to two or more hubs that connect to the same switch.

In addition, an ALB team provides fault tolerance for the network connection, but because both adapters connect to the same switch, like an AFT team, if the switch fails, network connectivity is lost.

## Configuring Power Inputs

Irrespective of the amount of resources in your system and fault tolerant configurations, if your system loses power, not only will its resources be unavailable, but you may also lose or corrupt data. When the server is running multiple virtual machines, sudden loss of power to the server will have a critical impact on your network infrastructure.

To protect the system against power outages, so that it can continue processing or shut down gracefully and minimize the likelihood of data loss or corruption, you must connect the server to an uninterruptible power supply (UPS).

For the Guide scenario, you will connect the FT server to two separate power supplies to provider greater fault tolerance.

Connect your server to the power supplies as follows:

1. Locate two black power cords and two labels, **A** and **B**.
2. Attach an **A** label to one power cord and a **B** label to the other.
3. Connect one end of cable **A** to the receptacle on one of the **modules.** Connect the other end to the **UPS**.

*Make sure that the power interlock mechanism is unlocked when you insert the power cord.*

4. Connect one end of cable **B** to the receptacle on the **second module**. Connect the other end to a second, separate power source.
5. At the front of the system, make sure that you fully insert the **modules** in the **shelf unit** by tightening the **thumbscrews**, if necessary. Then, at the rear of the system, turn the **power interlock mechanisms** into the **locked** position.

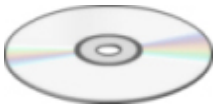
Now that you have constructed your hardware platform, you can configure the operating system to utilize the FT Server's fault tolerant capabilities.

For more information about correctly locating your server in your rack, see the *FT Server Site Planning Guide* on the NECAM website:

http://support.necam.com/servers/ft/320Ma/NR573.pdf

For more information about server installation and power requirements, see the *FT Server System Installation Guide* on the NECAM website:

http://support.necam.com/servers/ft/320Ma/NR575.pdf



# STEP 2: Install the Operating System

It is important that the operating system and the FT Server interact effectively to provide your virtual solution with all fault tolerant capabilities. Because the NEC Virtual Server 2005 R2 SP1 solution gains its fault tolerance from the hardware configuration, it is important that you install the necessary NEC hardware drivers and utilities to enable the fault tolerant capabilities of the server.

NEC FT servers are designed to deliver complete system redundancy. Memory, processors and Input–Output components are all redundant, which helps to eliminate potential failure points and ensure data is continually processed and not lost. This active lockstep processing delivers sustained system integrity to the operating systems and applications by ensuring continuous processing – even in the event of a hardware failure.

To install hardware support to enable this functionality, use the NEC ExpressBuilder CDs to perform the initial program load. The NEC ExpressBuilder CDs contain customized drivers that are required to run an FT Server optimally.

The following two procedures are necessary to install the operating system, associated drivers, and utilities on the FT Server:

- Initial program load (IPL)
- Post initial program load (Post-IPL)

NEC engineers typically complete the IPL procedure before you receive the server, which completes installation of the following:

- Operating system files and customized drivers specific to NEC Fault Tolerant Servers.
- Microsoft Windows Server 2003 Enterprise Edition with Service Pack 1.
- NEC Fault Tolerant Server software, including ftServer drivers, ftServer Manager, and Software Availability Manager (SAM).
- Java™ Runtime Environment (JRE) for the Virtual Technician Module (VTM) console.
- System documentation.

The post-IPL procedure includes:

- Installation programs for third-party software. It is important to install the third-party software, because NEC does not support systems where installation of this software has not taken place.

This Guide assumes the IPL procedure is complete for the system you want to use, so you only need to complete the post-IPL procedures.

## The Post-IPL Procedure

To complete the post-IPL procedure:

1. Turn on the **FT Server**.
2. Using the **Welcome to the Windows Setup Wizard**, provide the relevant information for **regional settings**, **names**, and **passwords**. When this **Mini-Setup** is finished, the system restarts.
3. When the **Welcome to Windows** dialog box appears, press the **CTRL+ALT+DELETE** keys.
4. Log on by using the **Administrator** account and the **password** that you entered during the **Mini-Setup**, and then click **OK**.

5. Two separate **End User Licensing Agreements (EULAs)** appear. Read the agreements and click **Continue** for both of them to install the software.
6. The installation programs for **third-party software** run after you click **Continue**. You must install the software, because NEC does not support servers that lack this software.
    a. When the **Java Runtime Environment (JRE) Wizard** starts, follow the prompts to install the **JRE**, and accept the **license agreement** and the **default settings** in the remaining dialog boxes. (If the progress bars partially obscure the **JRE Setup** dialog box, click the **JRE Setup** dialog box to bring it forward.)

*If the **Setup Complete** dialog box for any **third-party software** appears, click **No, I will restart my computer later**, and then click **Finish**. If you restart the system now, the installation does not complete properly.*

7. When **Setup** displays the **IPL Completed** dialog box, click **Restart**.
8. Restore the **default BIOS** settings to enable **boot monitoring** and to enable **Option ROM** on the **PCI slots**. While the system is starting, press **F2** to enter the **BIOS Setup program**. In the **BIOS Setup program**, press **F9** to restore the **default settings**, and then press **F10** to exit from the **BIOS Setup program**. You must **enable boot monitoring** to maintain fault tolerance.

*Make sure that you **enable boot monitoring** or you will compromise the fault tolerance of the system. The **IPL Procedure** turns off **boot monitoring**.*

9. After the system has restarted, **log on**. The **Post Installation Check** window appears for several minutes.
10. The **Post Installation Check Tool** dialog box appears and runs automatically. This tool verifies that the install was successful. Click **Exit** to dismiss the **Post Installation Check Tool** dialog box.
11. The **Has the NEC ExpressCluster Web service been set up?** message box may appear during the **NEC ExpressCluster SRE** installation, but it will automatically disappear after 5 seconds. **DO NOT** react to this prompt, or the system may appear to hang.

The IPL and post-IPL procedures install the drivers and utilities that are necessary for the server to operate and fail-over successfully. However, neither process configures other fault tolerant components, such as disk mirroring and network adapter teaming. It is necessary to complete these configurations after the post-IPL procedure completes. *STEP 3: Configure the Server Hardware* describes these procedures.

## Using Group Policy to Disable Automatic Updates

The installation of updates from the Microsoft Windows Update site may introduce compatibility problems with the FT Server. For this reason, you should disable Automatic Updates and install all updates from the NECAM support website. To ensure that this setting is persistent, you must put your FT Server in an organizational unit in Active Directory and apply a Group Policy that disables Automatic Updates.

To configure Group Policy to disable Automatic Updates:

1. Create a new **organizational unit** for the **FT Server** and move the server into it.
2. Open **Group Policy Editor** for the **organizational unit** that contains your **NEC Fault Tolerant Server**.
3. Navigate to **Computer Configuration\Administrative Templates\Windows Components\Windows Update.**
4. In the **right-hand pane**, double click **Configure Automatic Updates** and set the value to **Disabled**. Figure 5 shows this setting.
5. Click **OK**.
6. Close **Group Policy Editor**.

7. Open a **Command Prompt Window**, type **gpupdate** and press **ENTER**. Confirm the policy success message.
8. Close the **Command Prompt Window**.

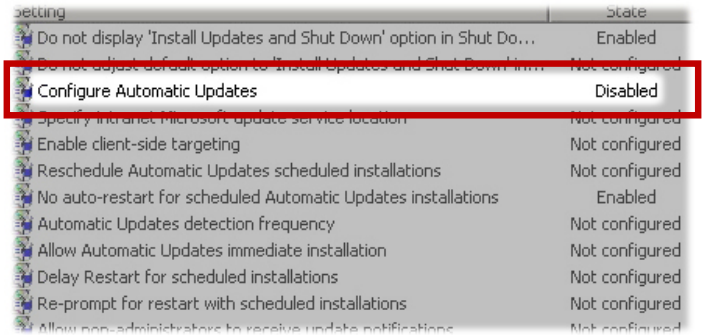



**Figure 5: Automatic Update setting in Group Policy.**

## Configuring Windows for Virtual Server 2005 R2 SP1

When the operating system installation is complete, configure a number of settings to enable Windows to provide the best environment for your virtual solution. To configure Windows to create an optimal environment for Virtual Server 2005 R2 SP1, consider the following:

1. Do not use the **/3GB** in **boot.ini** switch to alter Windows memory allocation. For Windows to optimize the running of the virtual machines, leave the default system memory allocation.
2. Configure **processor scheduling** (Background Services) and **memory usage** (System Cache) as follows:
    a. In **System Properties**, on the **Advanced** tab, in the **Performance** section select **Settings**.
    b. In **Performance Options**, select the **Advanced** tab.
    c. Configure the settings as shown below.

Figure 6 shows how you should configure the settings on the **Advanced** tab.

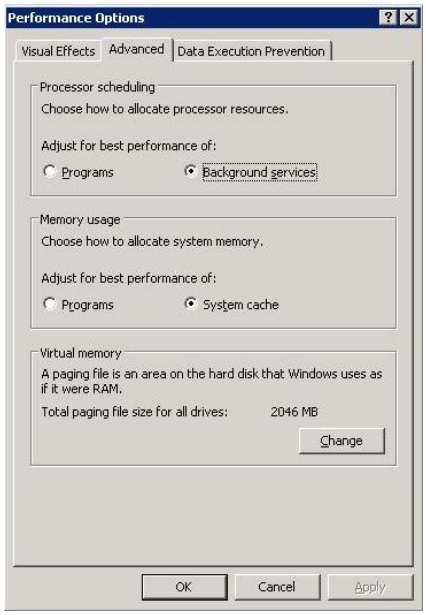



**Figure 6: Advanced tab in Performance Options.**

3. Exclude virtual machine files, especially **hard disk files (.vhd)**, from **virus-scans** and **real-time scanning** because this affects performance. In addition, install the standard **anti-virus protection** of your organization into each **virtual machine** to protect the virtual machine directly.

After you install Windows and the necessary NEC drivers and third-party utilities, you must configure fault tolerance for the components that the IPL and post-IPL procedures do not configure. Specifically, you must configure fault tolerance for the network connection and hard disks.

# STEP 3: Configure the Server Hardware

The FT Server is set up in an active\stand-by configuration after the IPL and post-IPL procedures. However, you must configure redundancy for network connectivity and hard disks separately.

When you create any fault tolerant system, it is important to understand that hardware faults *will* occur and to plan accordingly. The best way to deal with the issue of hardware faults is to configure systems to fail-over to an operational system or maintain functionality in the event of a component failure.

## Disk Mirroring

To provide fault tolerance for internal disks, including the system disk, configure disk mirroring. Create logical drives on the mirrored disks for the virtual machine files.

Table 1 shows the disk configuration for the Guide solution.

| Server Virtual Disk | Logical Drives | Storage Type | Virtual Machines |
|---|---|---|---|
| 1 | 1 | System Disk | 0 |
| 2 | 2 | Virtual Machine | Domain Controller<br>File Server |
| 3 | 1 | Virtual Machine | Email Server |

**Table 1: Disk configuration.**

For optimal performance, you can use Rapid Disk Resync (RDR) disk mirroring to configure and create managed disks in the internal storage enclosure of the FT Server. Internal disks are the only disk configuration that supports RDR disk mirroring. With RDR disk mirroring, you mirror pairs of physical disks to create virtual disks. Each pair of mirrored disks constitutes one virtual disk. The storage subsystem replicates the data on one disk to the corresponding disk. RDR disk mirroring does not create volumes; you must create volumes by using Disk Management within Windows.

Before you start this step, ensure that the second hard disk (the one designated as the mirror) has no partitions. You should also make sure that both of the disks that you are mirroring are similar in the following ways:

- Both have the same capacity (if they have different capacities, you must add the disk with the smaller capacity to the virtual disk before you add the disk with the larger capacity).
- Both are basic disks (not dynamic).

To mirror the disks, complete the following steps for each virtual disk in the solution:

1. Insert and latch disks into **corresponding slots** in each **module** of the server.
2. On the **Windows Desktop**, double-click **ftServer Management Tools** to start the **ftServer Management Console (ftSMC)**.
3. In **ftSMC**, select the disk you are going to mirror in the **I/O enclosure**. To do this, expand **ftServer I/O Enclosures**, **I/O Enclosure – x(10 or 11)**, **Storage Enclosure – x(10 or 11)**, and **Slot - 1**, and then click **Disk - 0**.

4. **Right-click** the disk that you **will join to the mirror** and click **Add Physical Disk To RDR Virtual Disk**.

Figure 7 shows Step 4 of adding a physical disk.

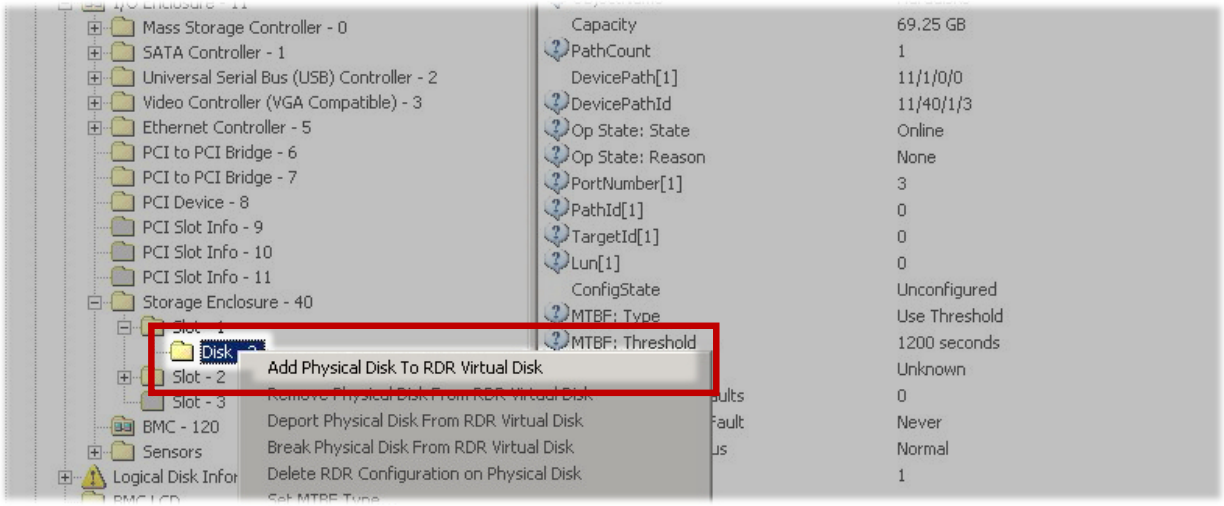



**Figure 7: Adding a physical disk.**

5. In the **Device Configuration Change** message box, click **Yes**.
6. Repeat Steps 4–6 on the corresponding disk in the other **I/O enclosure**. For example, expand **ftServer I/O Enclosures**, **I/O Enclosure - 11**, **Storage Enclosure - 40**, and **Slot - 1**, and then click **Disk - 1**.
7. Allow time for the two disks to synchronize.

*To synchronize the **system disk**, use the same process but locate the **CPU-I/O** enclosure bay that indicates **Unconfigured System Disk** in Step 3.*

While the disks are re-synchronizing, LEDs blink to indicate read and write operations, and in the details pane for the disk, **ftSMC** displays a value of **Syncing** next to **OpState: State**.

To view the progress of the synchronization in **ftSMC**, under **ftServer I/O Enclosures** expand **Logical Disk Information** and select the **virtual disk**.

Figure 8 shows a re-synchronization in process.

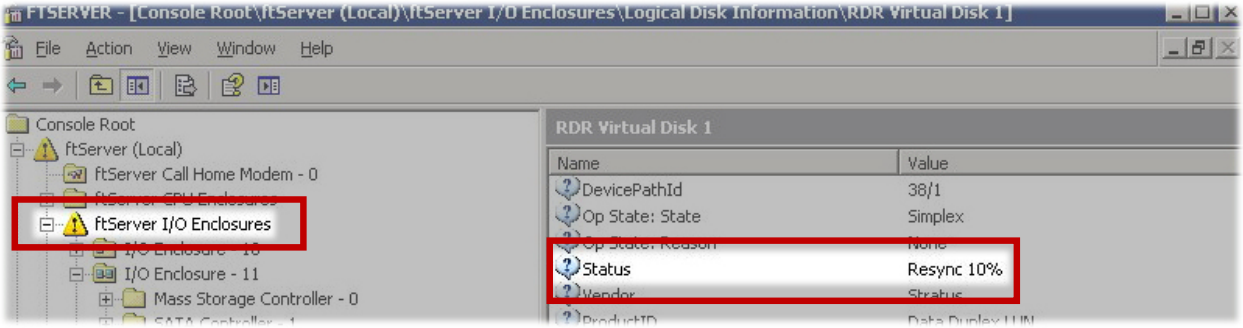



**Figure 8: Disk re-synchronization.**

After synchronization, the LEDs on both disks show a **steady green light** and, in the details pane for the disk and for the virtual disk, **ftSMC** displays a value of **Duplex** next to **OpState: State**. The value next to **Status for the virtual** disk is **None**.

When you add the **first system** disk to an **RDR virtual disk**, a **System Shutdown** message appears, which states that the **system will reboot in two minutes**. Let the system restart.

## Network Adapter Teaming

Configure teams of network adapters to increase the redundancy and capacity of a network connection. Before you configure the teams, you should attach the network adapters to the network. The Guide describes this process in *STEP 1: Install the Hardware*.

***Important**: FT Servers **DO NOT** support **Express Teams**. Create only **Advanced Networking Service Teams** by using the **PROSet utility**.*

You will create an Adapter Fault Tolerant team for the virtual machines to use to connect to the network. The team will use two of the four installed network adapters. You may use the additional adapters later to provide connectivity for additional virtual machines or to distribute the network load.

To configure network adapter teaming, complete the following steps:

1. Start the **PROSet utility** and in the **notification area**, double-click **PROSet**.
2. In the **Intel® PROSet for Wired Connections** dialog box, **right-click** one of the **Ethernet** ports listed, point to **Add to Team**, and then click **Create New Team**. The **Teaming Wizard** starts.

Figure 9 shows this path for Step 2.

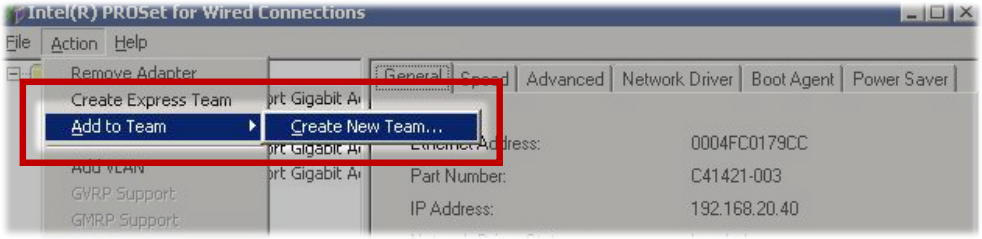



**Figure 9: Creating a new adapter team.**

3. In the first dialog box of the **Teaming Wizard**, select **Adapter Fault Tolerance** and click **Next**.
4. In the next dialog box, select the **adapters** for the team. A **check mark** next to an adapter indicates that the adapter will become a member of the team. Select the **check boxes** next to the adapters to turn on or turn off the required team members. Make sure that you create teams that contain adapters that are located in different modules (typically adapters 1 and 3 are teamed and /or adapters 2 and 4 are teamed). One way to determine where adapters are located is to use the **Identify Adapter** utility in **PROSet** to flash the LED on each adapter. In **PROSet**, click the adapter, on the **General** tab, click **Identify Adapter** and follow the instructions in the **Identify Adapter** message box.

Figure 10 shows the Teaming Wizard settings.

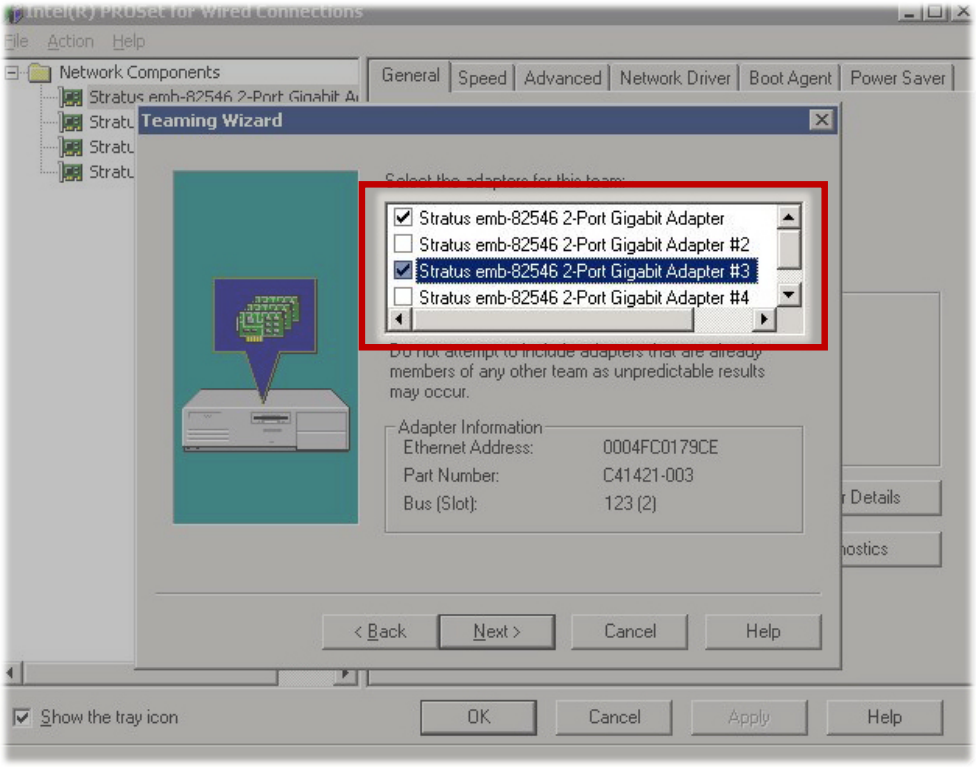



**Figure 10: Select adapters for team.**

*If you add adapters to a team later, the system briefly loses network connectivity. To avoid this network interruption, configure a larger team now.*

5. Click **Next** and click **Finish**.
6. When the **Intel® PROSet for Wired Connections** dialog box reappears, click **Apply**. **PROSet** binds the specified adapters into teams.

*This operation takes at least one minute per team to complete. PROSet closes after processing is complete. Do not abort the operation until it has completed, otherwise you must repeat the procedure.*

After you have finished configuring fault tolerance for your FT Server, you will install Virtual Server R2 SP1.


# STEP 4: Install and Configure Virtual Server 2005 R2 SP1

Installing Virtual Server R2 SP1 on a computer enables the computer to become a host for virtual machines. The configuration and management of virtual machines uses the Virtual Server Web application. You can install the Web application on the virtual server or on a separate management Web server to enable remote management for the virtual machines. If you install the Web application on a separate Web server, you will gain the following benefits:

- You maximize the resources that the Virtual Server can use for the virtual machines.
- You reduce the attack surface for the Virtual Server host system by not installing Internet Information Services (IIS).
- You can automatically launch Windows updates on the system running the management Website (you disable them on the virtual server).

For these reasons, we recommend that you install the Virtual Server Web application on a separate management Web server.

Figure 11 shows the installation of the Virtual Server Web application on a separate system.

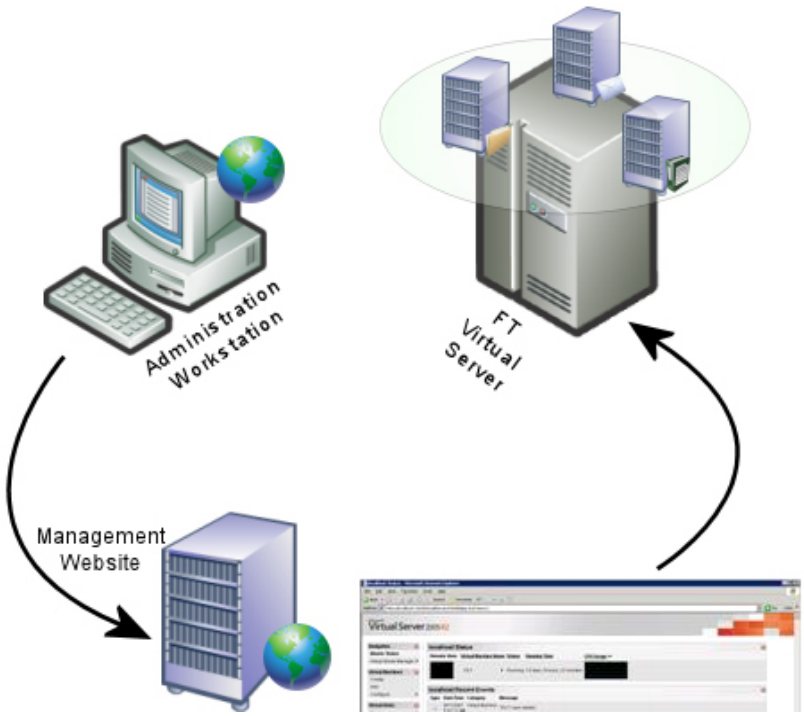



**Figure 11: Remotely managing virtual machines.**

The installation of the Web application on a separate management system requires that you do the following:

- Configure Constrained Delegation for the management system account in Active Directory.
- Run a custom installation of Virtual Server and choose to install only the Web application.

## Installing Virtual Server

You install Virtual Server R2 SP1 on the FT Server without installing the management Web application.

1. From the **Virtual Server CD-ROM,** start the **Setup Wizard (also called Microsoft Virtual Server 2005 Setup)**. If you start the **Setup Wizard** manually, use **Setup.exe**.
2. Proceed through the wizard until you reach the **Setup Type** page.
3. On the **Setup Type** page, select **Custom**.
4. Click **Virtual Server Web Application** and select **This feature will not be available**. Figure 12 shows this interface.

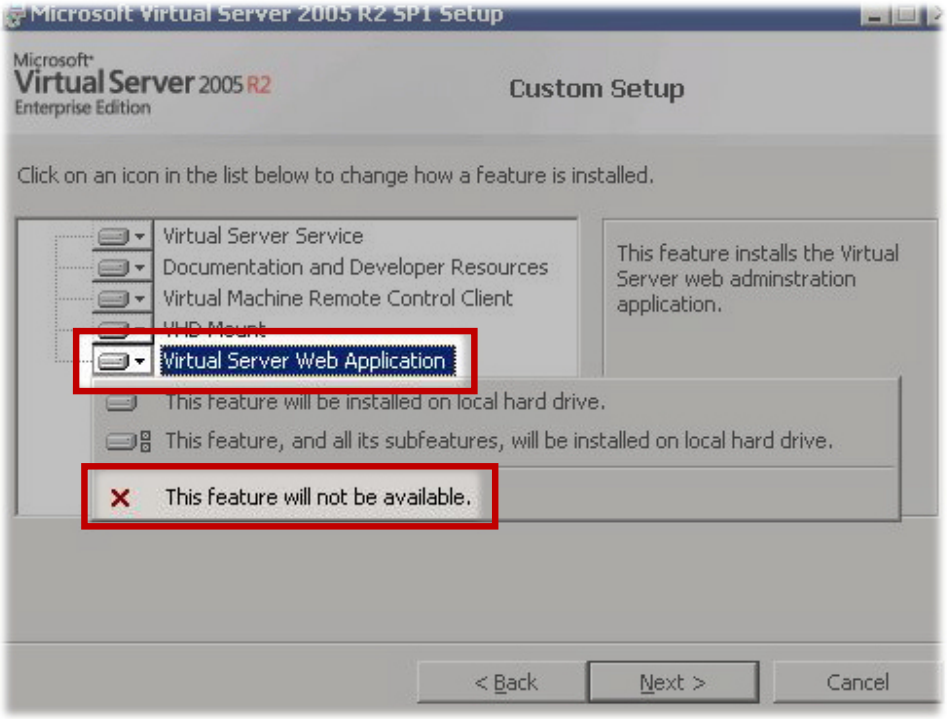



**Figure 12: Deselect the Virtual Server Web Application**

5. Accept the **defaults** in the installation wizard.
6. Click **Install** to begin the installation.
7. Once the installation is complete, the **Setup Complete** page appears. Click **Finish** to close the page and exit the **Setup Wizard**.

## Virtual Server Web Application

Install the Virtual Server Web application on a management system to create a management website. To enable the Web application to manage virtual machines on a remote system, configure Constrained Delegation. Constrained Delegation enables the Web server to forward client credentials to the host Virtual Server to enable the client to manage the virtual machines.

Before you configure Constrained Delegation, ensure the domain functional level is Windows Server 2003 native. Complete the following steps to configure constrained delegation:

1. On the **domain controller**, open **Active Directory Users and Computers**.

2. In the **console tree,** click **Computers**.
3. Right-click the **Web server** that will run the **management Website** and click **Properties**.
4. On the **Delegation** tab, click **Trust this computer for delegation to specified services only**.
5. Click **Use any authentication protocol**.
6. Click **Add**, and then click **Users and Computers**.
7. Type the **name of the computer** running the **Virtual Server service**, and then click **OK**.
8. From the list of **available services**, hold down the **CTRL key** while clicking **cifs** and **vssrvc**, and then click **OK**.

To install the Virtual Server Web application on a separate system that is running the management website:

1. On the computer on which you intend to install the **Administration Website for Virtual Server**, from the **Virtual Server 2005 CD-ROM** start the **Virtual Server Setup Wizard**. If you start the **Setup Wizard** manually, use **Setup.exe**.
2. Proceed through the wizard until you reach the **Setup Type** page.
3. On the **Setup Type** page, select **Custom**, and then click **Next**.
4. Click **Virtual Server Service**, select **This feature will not be available**, and then click **Next**.
5. On the **Configure Components** page, accept the default **Website port** value of **1024**.

Figure 13 shows this interface.

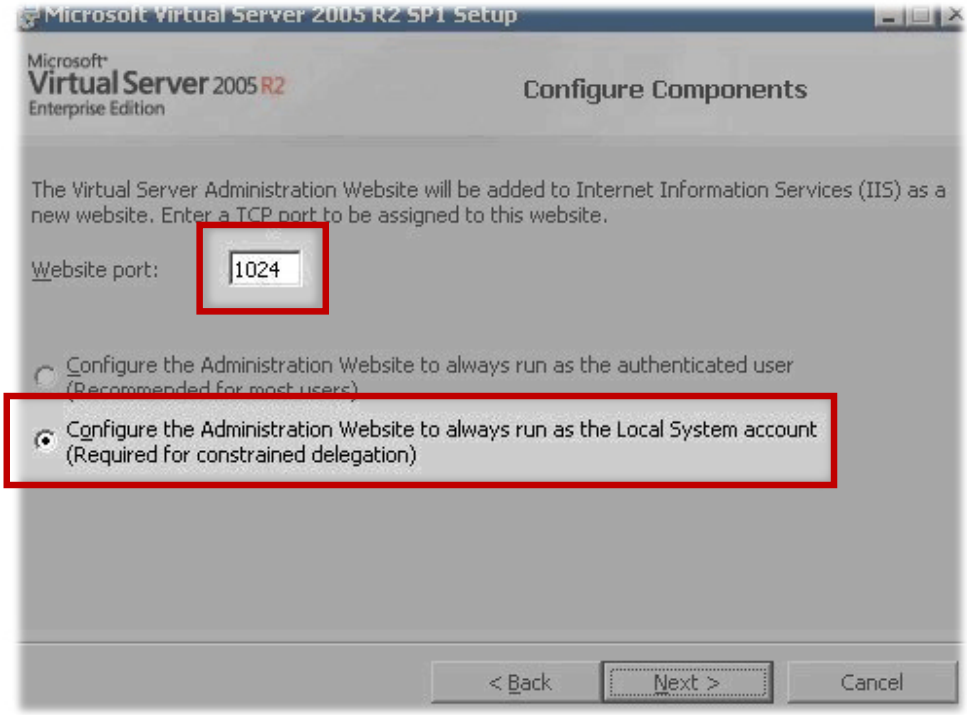



**Figure 13: Configure the Virtual Server Web Application port.**

6. Select **Configure the Administration Website to always run as the Local System account**, and then click **Next**.
7. Click **Install** to begin the installation.

8. Once the installation is complete, the **Setup Complete** page appears. Click **Finish** to close the page and exit the **Setup Wizard**.

After you install Virtual Server R2 SP1 on the FT Server and the management Website on a separate system, you now can deploy the virtual machines to the FT Server.

# STEP 5: Installing and Configuring the Guest Virtual Machines

After you install Virtual Server R2 SP1, you need to deploy virtual machines. You must run the virtual machines from the disks that you mirrored in *STEP 3: Install the Server Hardware* to gain the benefits of the fault tolerant disks.

The Guide solution virtualizes the following physical servers:

- Domain controller
- File server
- Email server

After virtualization, the physical servers will be decommissioned.

There are three approaches to deploying the virtual machines. These are:

- Build the virtual machine on the production virtual server and install software manually.
- Build the virtual machine on a remote virtual server and copy the virtual machine files to the production virtual server.
- Migrate physical servers to virtual machines by using a physical to virtual (P2V) process.

You can build the virtual machines directly on the production virtual server by using standard installation media. You must then replicate or restore data to the virtual machine. If the virtual machine is remote to the replication or backup source, the data must travel across the wide area network (WAN).

Alternatively, you can initially create the virtual machine in a separate location, such as a remote site. This enables you to replicate or restore data locally before deploying the virtual machine to the production virtual server. You can create a virtual machine on any virtual server and, because the virtual server virtualizes the underlying hardware for the virtual machine, you can copy that virtual machine to any other virtual server. This is useful for building a production environment in situations where it is easier to build the virtual machine in a separate location to the final, operational location.

Figure 14 shows this process.

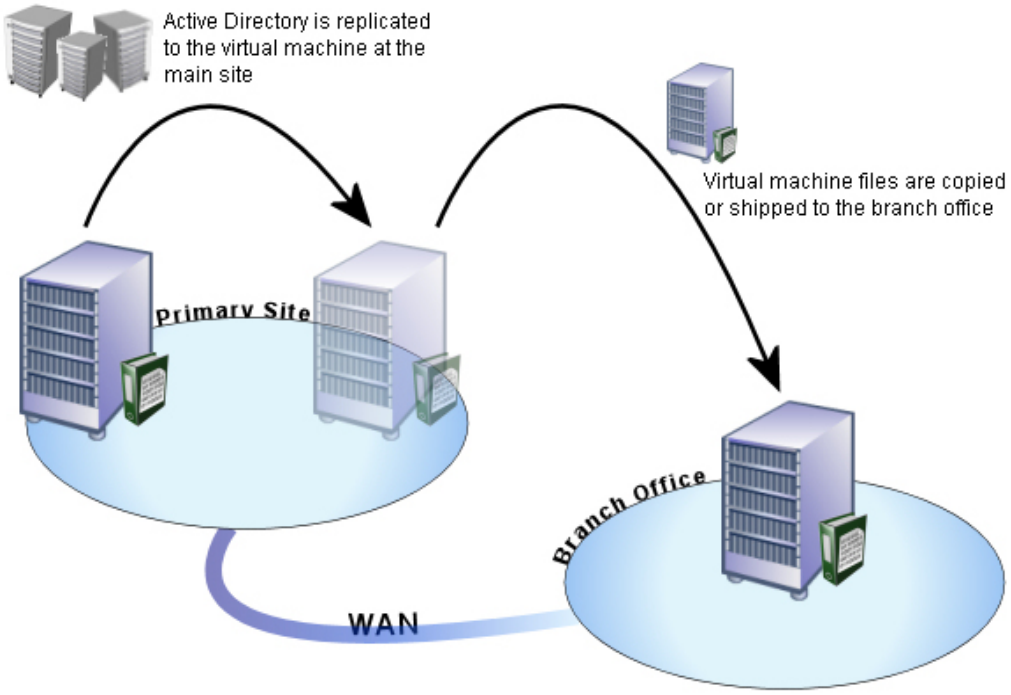



**Figure 14: Building a guest machine at the main site and transporting it to the branch office.**

The P2V migration of a physical server to a virtual machine enables you to deploy a virtual machine that replaces a physical server if rebuilding the server from scratch would be difficult because of specific software installation or configuration. In addition, the P2V process can streamline the creation of multiple virtual machines and prevent the need to undertake multiple new manual virtual machine builds. The *Virtual Server Migration Toolkit (VSMT)* describes how to complete the P2V process.

Table 2 summarizes these approaches.

| Virtual Machine Deployment Method | Advantages | Disadvantages |
|---|---|---|
| Build new virtual machine and install all software manually | Enables straightforward creation of virtual machines. | Time consuming build process.<br>Remote replication of data.<br>Identification of software configuration requirements. |
| Build the virtual machine on a remote Virtual Server and copy the virtual machine files to the local Virtual Server | Uses a virtual machine template.<br>Replicates data locally before deployment. | Must move large virtual machine files.<br>Identification of software configuration requirements. |
| Migrate a physical server to a virtual machine by using a P2V process | Migrates configuration from the physical server.<br>Original installation media may not be required.<br>Once the infrastructure is in place it can significantly reduce migration times. | Intricate process with many steps.<br>Requires Automated Deployment Services (ADS) 1.0 and Windows Server 2003, Enterprise Edition.<br>All applications are migrated, even those that may not be required. |

**Table 2: Creation options for virtual machines.**

For more information on the P2V process and the VSMT, see:

http://www.microsoft.com/windowsserversystem/virtualserver/overview/vsmtwhitepaper.mspx

In addition, third-party vendors provide P2V utilities that you can use for migrating physical servers to virtual machines, including:

PlateSpin – http://www.platespin.com

Portlock – http://www.portlock.com

Acronis – http://www.acronis

Due to the proprietary nature of these P2V solutions, this guide focuses on the process of building new virtual machines that you use to replace the physical hardware. This approach provides the best solution in this scenario because there is no need to replicate data from a remote, bandwidth-constrained site.

## Resource Assignment

As with physical servers, you should provide enough physical resources to the individual virtual machines to gain optimal performance. The resources you can allocate are limited to the actual physical resources that are available in the physical virtual server host system. Therefore, it is important to understand the levels of resource usage you can expect from the virtual machines before you build the physical host system.

To identify the level of resources to assign to each virtual machine, you can monitor the physical computers you intend to virtualize and identify the memory and processor utilization. Use this as a minimum level to assign to the virtual machine. The following examples illustrate minimum levels:

- A server with 40 percent memory utilization in a 1 GB system requires at least 400 MB of RAM.
- A server with 70 percent CPU utilization in a 1 GHz system requires at least 0.7 GHz of processor cycles or the equivalent of a 700 MHz processor.

These calculations can never be completely accurate but provide a minimum resource requirement for your physical server and therefore your virtual machine. It is best practice to ensure that the physical server has enough resources by allocating approximately 50 percent more than the minimum that you determine is necessary to support all your virtual machines.

In addition, you must identify how much physical disk space the virtual machine requires for its virtual disks. It is a best practice to create a fixed-size virtual disk that has enough space for data expansion. Virtual disks that expand dynamically take a very high percentage of system resources when they expand, so you should not use them in a production environment. Each virtual disk must have enough space for the guest operating system and applications in addition to the data it must hold.

Table 3 shows the virtual machine resource allocation.

| Virtual Machine | Role | Memory Allocation | Disk Allocation | CPU Allocation |
|---|---|---|---|---|
| DC1 | Domain controller | 0.5 GB | 100 GB | 0.7 GHz |
| FS1 | File server | 1.0 GB | 300 GB | 1 GHz |
| EX1 | Email server | 1.5 GB | 300 GB | 1.2 GHz |

**Table 3: Virtual machine resource allocation.**

Table 3 shows that the virtual machines require a total of 3 GB of RAM, 700 GB of disk space, and a 3 GHz processor. You must add to these amounts the host physical server resource requirements so that you can calculate the resource requirements for the solution.

Table 4 shows the total physical server resources for the Virtual Server host computer.

| Memory Allocation | Disk Allocation | CPU Allocation |
|---|---|---|
| 8 GB | 1500 GB | 2 x 3 GHz |

**Table 4: Host server resource allocation**

## Creating the Virtual Machines

When you create a virtual machine instead of adding an existing virtual machine, you must assign a virtual hard disk to it and install an operating system on the virtual hard disk. This process will vary with the requirements of each installation. However, there are a number of key stages to ensure a smooth migration to a virtual machine environment. The first step is to create the Virtual Machine settings on the Virtual Server.

**To create a new virtual machine:**

1. On the system that is running the **management Website**, open the **Administration Website**.
2. In the **navigation pane**, under **Virtual Machines**, click **Create**.
3. In the **Virtual machine name** box, type a name for the virtual machine and specify a **fully qualified path** to the location where you want to create the **virtual machine hard disks**.

   *Note: For this Guide, we have used a simplified naming standard for clarity; we recommend you use a naming standard that is appropriate for your organization.*
4. In the **Virtual machine memory box**, type the **required memory allocation** in **megabytes**.

   *Note: If you allocate more memory to virtual machines than is available in the virtual server the virtual machines will not start.*
5. In the **Virtual hard disk** box, select **Create a new virtual hard disk**.
6. To set the **size** of the **virtual hard disk**, specify a value in the **Size** box.
7. Under **Virtual network adapter**, in **Connected to**, select the network adapter team.
8. Click **Create**.

Repeat this process for each of the servers that you migrate to the virtual server. Once you have created these virtual machine settings you can build each virtual machine. The Guide uses the following virtual machines:

- Domain controller (DC1)
- File server (FS1)
- Email server (EX1)

The following checklists provide the key stages in the virtual machine creation process. The checklists highlight the important information and steps that you must take to complete the creation of each virtual machine.

### Virtual Machine Additions

Virtual Machine Additions is a set of features that improves the integration of the virtual server and virtual machine operating systems. It also improves the performance and manageability of the virtual machine operating system. You must install Virtual Machine Additions after you install the operating system on the virtual machine and restart Windows on the virtual machine after installation.

To install Virtual Machine Additions:

1. On the **Master Status** page, click the **arrow to the right of the virtual machine** and select **Edit Configuration**.
2. Select the link to start **Virtual Machine Additions setup**.

3. Complete the **Installation Wizard**.

It is good practice to install Virtual Machine Additions as soon as possible after you complete the initial operating system installation. In the following section, each checklist indicates the recommended point that you can install the Virtual Machine Additions during the build process or each VM.

## Domain Controller (DC1) Build Checklist

You can replicate the directory data for a new domain controller virtual machine from an existing domain controller in your organization. Therefore, the simplest approach you can take for the DC1 installation is to setup a fresh installation with the domain controller server role. The standard domain replication process will then populate the domain controller information from the existing domain controllers in the Enterprise. The key checkpoints for building your domain controller virtual machine are:

**Creating the new domain controller:**

- Check a domain controller is available on the network; this can be the physical domain controller for migration.
- Insert your Windows 2003 Server CD into the FT Server CD-ROM drive and, using the Virtual Server Administration website, turn on the DC1 virtual machine and remote control it.
- Complete a standard Windows Server 2003 installation. Use a unique server name and IP address using your organizations naming and numbering standards.
- Install Virtual Machine Additions.
- Using **Windows Update**, install the latest service pack and updates to the DC1 virtual machine.
- Add the **Domain Controller (Active Directory)** server role to DC1. For guidance on this process, see the **Domain controller role: Configuring a domain controller** topic in the Windows Server 2003 **Help and Support Center**.
- After the **Active Directory Installation Wizard** process has completed and the virtual machine restarts, check the DNS server to ensure that the DC1 virtual machine has registered its DNS records.
- After you complete the installation, check the DC1 event logs to ensure the server is functioning correctly. If errors are present, refer the Windows Server 2003 **Help and Support Center** for troubleshooting guidance.

Only after you confirm the DC1 virtual machine is functioning correctly should you start the process of decommissioning the physical domain controller.

**Decommissioning the old physical domain controller:**

- Use **Active Directory Users and Computers** to move the **Operations Masters** from the physical domain controller to DC1 or another physical domain controller as required.
- Remove the **Domain Controller (Active Directory)** server role from the physical domain controller. Ensure the **This server is the last domain controller in the domain** check box is **NOT** checked.

Once the **Configure Your Server Wizard** has completed and the physical server has rebooted you can safely decommission or reconfigure the physical server for reuse elsewhere in your IT infrastructure.

## File Server (FS1) Build Checklist

To migrate a file server role from a physical server to a virtual machine requires additional steps to ensure the configuration and user data is maintained. Typically, you use either the P2V process or a backup solution to

backup the data from the physical file server and restore it to the virtual machine. The exact process will vary greatly depending on the software your organization uses as a backup recovery solution. There are three basic approaches to this migration:

- **Bare metal restores**. If your backup and recovery solution supports a bare metal restore it is capable of performing a full system recovery in a single process. It is important that you verify that you will be able to access the backup volume set from within the virtual machine environment. As Virtual Server 2005 R2 SP1 does not support Plug and Play (PnP) buses such as USB and IEEE 1394 you will have to be able to access the recovery data via local hard drive, CD or DVD drive or over the network using pre-boot execution (PXE). You should discuss the options with the supplier of your backup and recovery solution before you plan to use this approach for the migration of your physical server.
- **Data and configuration recovery**. This approach requires you to install an operating system on the target system, which you use to launch the recovery process. The recovery process re-configures the operating system and restores data and applications.
- **Data recovery**. If you configure your recovery solution to backup the user's data only, you will have to configure the new operating system environment to match the physical file server before you will be able to restore the data. For example, you will have to create the required folders, shares, and access permissions before you restore the user data.

Whichever solution you use there are a few important steps that you should follow to complete the migration process:

**BEFORE you take the physical server offline:**

- Allocate sufficient time to complete a full backup of the physical file server.
- Ensure no users are able to change the data on the physical server during or after the backup completes.
- Record all relevant shares and permissions on the physical server to help with service validation after you restore FS1.
- Remove the physical file server from the domain and use **Active Directory Sites and Services** to replicate the removal of the computer object to all domain controllers.
- Rename the physical file server and take it offline before starting the migration process for the virtual machine.
- **DO NOT** remove any data from this server until you have confirmed the migration process has completed correctly on the FS1 virtual machine.

**AFTER the physical server is offline:**

- Use your organization's backup and recovery solution to complete a restoration of the file server configuration and data.
- Install Virtual Machine Additions.
- Ensure all user data, system configuration information, applications, and permissions are correctly restored to the FS1 virtual machine.
- After you have confirmed the successful migration of the server, you should ensure that you remove the old data securely from the physical servers' hard drives.
- **DO NOT** bring the physical server back online without re-installing the operating system. Failure to complete this step can cause problems if you attempt to join the physical server to the domain again.

## Email Server (EX1) Build Checklist

The email server migration uses a similar "side-by-side" approach to that used for the domain controller migration. The Exchange Server infrastructure and tools allow you to create a new Exchange Server and move

the users' mailboxes directly from the physical server to the virtual machine. This approach minimizes the downtime of the service for the users and provides the simplest recovery process in the event that the migration runs into problems. The key stages for building your email virtual machine are:

**Creating the new email server:**

- Insert your Windows 2003 Server CD into the FT Server CD-ROM drive and, using the Virtual Server Administration Website, turn on the EX1 VM and start a remote control session.
- Complete a standard Windows Server 2003 installation using a unique server name and IP address.
- Install Virtual Machine Additions.
- Use **Windows Update** to ensure your server has the latest service packs and updates.
- Install Exchange 2003 and apply the latest service pack and updates.
- Join EX1 to the existing Exchange organization.
- Move the user mailboxes from the physical email server to the EX1 VM. For guidance on this process, see the following Microsoft KB article: http://support.microsoft.com/kb/821829

After you have confirmed the EX1 virtual machine is functioning correctly, you can start the process of decommissioning the physical email server.

**Decommissioning the physical email server:**

- Remove the physical email server from the Exchange organization.
- Use the **Configure Your Server Wizard** to remove the physical server from the domain.
- Securely remove the data from the servers' hard drives.

After the **Configure Your Server Wizard** has completed and the physical server has rebooted you can safely decommission or reconfigure the physical server for reuse elsewhere in your IT infrastructure.

## Limit Virtual Machine Processor Usage

Because you have multiple virtual machines running on the same physical server and a finite amount of physical resources, you should ensure that an individual virtual machine is not able to use resources to the detriment of other virtual machines.

You can set limits on processor usage for each virtual machine, specifically:

- Relative Weight
- Reserved Capacity
- Maximum Capacity

**Relative Weight**
Virtual Server dynamically allocates a virtual machine with a higher relative weight additional resource as needed from other virtual machines that have lower relative weights.

**Reserved Capacity**
Virtual Server reserves this capacity of a single CPU for this virtual machine. The percentage of CPU capacity that is available to it will never be less than this amount.

**Maximum Capacity**

Virtual Server sets this value as the highest percentage of the total resources of a single CPU usable by this virtual machine at any given time.

*These settings relate to a single CPU. In Figure 15 you can see that the DC1 virtual machine has 100% Maximum Capacity (% of one CPU) and 50% Maximum Capacity (% of system) because there are two processors in the server.*

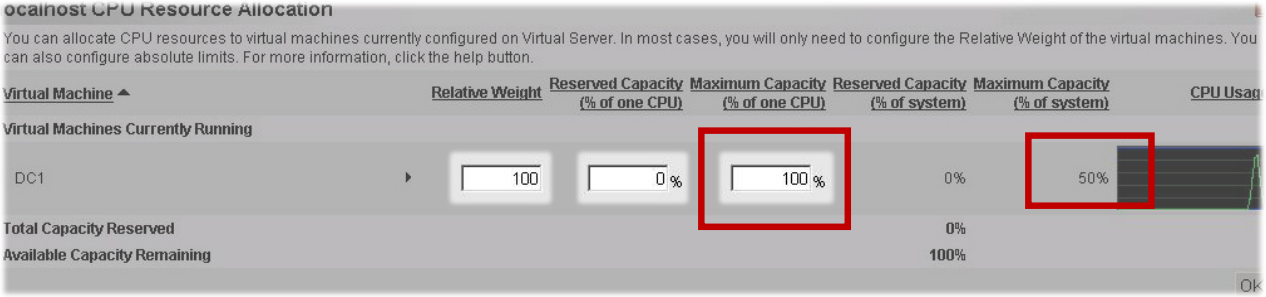



**Figure 15: Configuring processor utilization limits.**

For the scenario in this Guide, you leave the default processor allocations shown in Figure 15. The virtual server has sufficient hardware resources to run the three virtual machines comfortably.

## Configure Save State and Automatic Restart

To ensure that the virtual machines are operational when the virtual server service is running, (i.e. if the server is restarted), configure the virtual machines to save the current state when the virtual server stops and to automatically start when the virtual server starts.

To configure the Save state and Automatic restart options:

1. On the **Master Status** page, click the arrow to the right of the virtual machine and select **Edit Configuration**.
2. Click **General Properties**.
3. Type the **credentials** of a **domain account** for the virtual machine to run under. The account does not require special privileges, other than:
    a. On the .**vmc** file: **Read Data**, **Write Data**, and **Execute File**
    b. On the .**vhd** file: **Read Data**, **Read Attributes**, **Read Extended Attributes**, and **Write Data**
    c. On the .**vnc** file, if a virtual machine is connected to a virtual network: **Execute File**, **Read Data**, **Read Attributes**, and **Read Permissions**
    d. On the folder containing the .**vmc** file, for a virtual machine to have the ability to save state: **List Folder** and **Write/Create File**
4. Configure the virtual machine to **turn on automatically** when Virtual Server starts.
5. Configure the virtual machine to **Save state when Virtual Server stops**. Figure 16 shows you how to configure these settings.
6. Click **OK**.

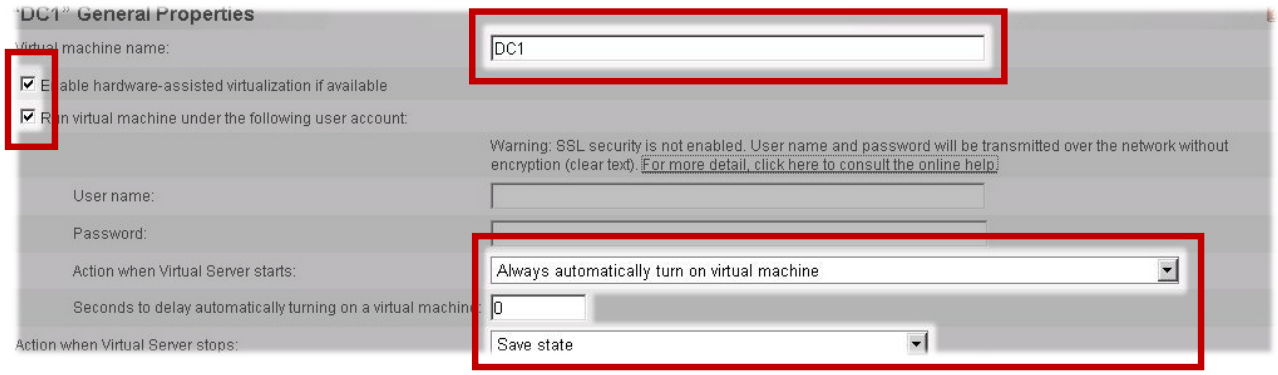



**Figure 16: Configuring virtual machine General Properties.**

The installation and configuration of your fault tolerant virtualization environment is now complete.

## Next Steps

You should closely monitor the virtual machines during the first few weeks of operation to ensure the correct configuration of your resource assignments. You can also use the Microsoft ® Windows Server ™ 2003 Performance Advisor tool to create performance baselines and reports for each virtual machine.

Use the tool inside each virtual machine individually to ensure that the baseline creation process does not introduce a significant load onto the host server. Get more information or download the free Server Performance Advisor 2.0 from the following URL:

www.microsoft.com/downloads/details.aspx?FamilyID=09115420-8c9d-46b9-a9a5-9bffcd237da2&displaylang=en

You have now been through the process of creating a resilient and reliable virtual server environment with NEC Fault Tolerant Servers and Virtual Server 2005 R2 SP1.

By following the recommendations, steps, and procedures in this guide you will create a flexible and robust virtualization environment for virtual machine-based production systems on your NEC Corporation of America Fault Tolerant Server (FT Server) platform.

# Additional Resources

If you have completed all of the procedures in this Quick Start Guide, your server is now configured to provide a high availability virtualization service. When you are comfortable with your new server, you can learn more about advanced performance and monitoring options, as well as some of the software features your server provides.

The following is a list of useful resources to help you to configure your server:

## The NECAM Online Server Support Guide

The first place to look for help is the NECAM website at:

http://support.necam.com/servers/ft

## The Microsoft Virtual Server Website

The Microsoft official Virtual Server Website is at:

http://www.microsoft.com/virtualserver

## Virtual Server Community

To find answers in Microsoft forums and newsgroups, locate non-Microsoft communities for Virtual Server, join in chats, and share best practices and tips with your peers, visit the Official Microsoft Virtual Server Community site at:

http://www.microsoft.com/technet/community/en-us/virtualserver/

Empowered by Innovation NEC


Windows Server System is comprehensive, integrated, and interoperable server infrastructure that simplifies the development, deployment, and management of flexible business solutions.
www.microsoft.com/windowsserversystem